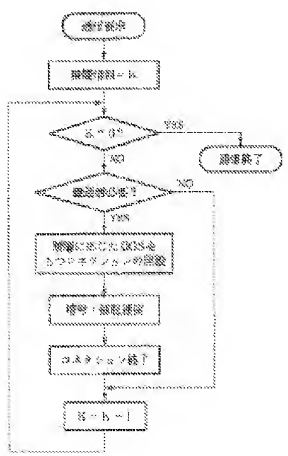
COMMUNICATION EQUIPMENT, SYSTEM AND METHOD

Publication number: JP10093547 (A)
Publication date: 1998-04-10
Inventor(s): IWAMURA KEIICHI +
Applicant(s): CANON KK +
Classification:
- international: ***H04L12/28; H04L9/08; H04L9/14; H04L9/32;*** **H04L12/28**; **H04L9/08**; **H04L9/14**; **H04L9/32**; (IPC1-7): H04L12/28; H04L9/08; H04L9/14; H04L9/32
- European:
Application number: JP19960243181 19960913
Priority number(s): JP19960243181 19960913

Also published as:
JP3630874 (B2)

Abstract of **JP 10093547 (A)**

PROBLEM TO BE SOLVED: To utilize a characteristic such as information and importance of service by providing a means that decides communication quality so that the quality of encryption and authentication communication relating to a higher layer is higher than the quality of encryption and authentication communication relating to a lower layer. SOLUTION: This equipment is composed of a QOS(quality of service) setting means conducting a QOS request setting means being a connection open realize means having QOS depending on each layer and a QOS storage means that receives hierarchical information and stores corresponding QOS as a table. On the occurrence of a communication request, at first highest quality QOS is requested and set based on hierarchical information K. The connection is in use and encryption and authentication communication is conducted with a highest master key.; After the encryption and authentication communication is finished, the connection is closed. Then the hierarchical information K is being decreased one by one and the connection depending on the layer is requested and set again and the operation is repeated and when K reaches 0, the communication is terminated.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－93547

(43)公開日　平成10年(1998)４月10日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00		６４１
9/08				６０１Ｚ
9/32				６７５Ａ
// Ｈ０４Ｌ　12/28			11/20	Ｄ

審査請求　未請求　請求項の数５　ＯＬ　（全　８　頁）

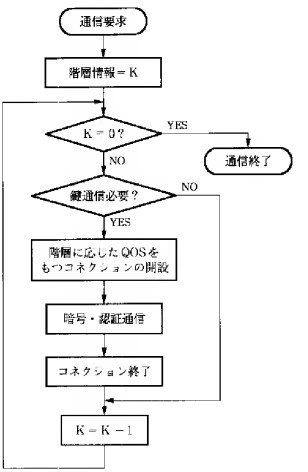
(21)出願番号　特願平8－243181

(22)出願日　平成８年(1996)９月13日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　岩村　恵市
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　弁理士　大塚　康徳　（外１名）

(54)【発明の名称】　通信装置及びシステム及び方法

(57)【要約】
【課題】　情報やサービスの重要度といった特徴を生かす通信を可能にする。
【解決手段】　階層的に構成され、上位階層に属する鍵が下位階層に属する鍵またはデータを変換して通信を行う暗号・認証による通信を行う場合に、上位階層に関する該暗号・認証通信の品質がそれより下位の階層に関する該暗号・認証通信の品質より高くする。



【特許請求の範囲】
【請求項１】　階層的に構成され、上位階層に属する鍵が下位階層に属する鍵またはデータを変換して通信を行う暗号・認証による通信通信であって、
上位階層に関する該暗号・認証通信の品質がそれより下位の階層に関する該暗号・認証通信の品質より高くなるように、通信の品質を定める手段を有することを特徴とする通信装置。
【請求項２】　更に、各階層毎の通信品質を任意に定める手段を有することを特徴とした請求項第１項に記載の通信装置。
【請求項３】　請求項１或いは請求項２のいずれかの通信装置によって構成されることを特徴とした通信システム。
【請求項４】　請求項１ないし請求項３のいずれかの通信の品質をＡＴＭ通信におけるＱＯＳとして定義されるパラメータとすることを特徴とした通信システム。
【請求項５】　階層的に構成され、上位階層に属する鍵が下位階層に属する鍵またはデータを変換して通信を行う暗号・認証による通信方法であって、
上位階層に関する該暗号・認証通信の品質がそれより下位の階層に関する該暗号・認証通信の品質より高くなるように、通信の品質を定める手段を有することを特徴とする通信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、動画像データ、静止画像データ、音声データ、コンピュータデータ等の情報を伝送するマルチメディアネットワークにおける通信装置、システムおよび方法に関するものである。
【０００２】
【従来の技術】次世代の基幹系通信インフラとして検討されているＢ－ＩＳＤＮ（BroadbandAspects of Integrated Services Digital Network：広帯域サービス総合ディジタル網）は、現在施行されているＩＳＤＮに比べ、伝送容量が大きく、かつ、（ネットワーク資源の許す限り）要求された伝送容量で通信サービスを提供することができる、柔軟なネットワークである。この様なサービスが可能なのは、一重にＡＴＭ（Asynchronous Transfer Mode：非同期転送モード）と呼ばれる、Ｂ－ＩＳＤＮの基幹技術によるものである。ＡＴＭでは、パケット交換伝送モードと同様に、宛先の書かれたラベルを格納したヘッダを付与した固定長のセルを送出することで任意速度に対応し、そのラベルを読むことで、交換機がスイッチングする。パケットが、固定長のセルという単位で構成されることで、物理層レベルでは高速同期通信が行え、パケット送出密度により任意の転送速度を確保できる。
【０００３】一方、このような通信インフラをユーザが安心して使えるためには、暗号・認証等のネットワークセキュリティ技術を必要とする。この暗号や認証は送信者と受信者で同一の暗号鍵を秘密に共有する共通鍵暗号方式（秘密鍵暗号方式、対称暗号方式、慣用暗号方式とも呼ばれる）や、暗号鍵と復号鍵が異なり、暗号鍵を公開、復号鍵を秘密に保持する公開鍵暗号方式によって実現できることが知られている（各暗号方式の詳細は池野，小山著「現代暗号理論」電子情報通信学会、１９８６．参照）。また、この様な鍵を安全に配送する方式に対しても種々の鍵配送方式が提案されている（たとえば辻井，笠原著「暗号と情報セキュリティ」昭晃堂，１９９０．参照）。以上のような技術を用いることによって、Ｂ－ＩＳＤＮに対しても安全な通信を実現することができる。
【０００４】
【発明が解決しようとする課題】上述のような暗号・認証通信においてはその安全性を高めるために図６に示すように鍵を階層化して用いる場合が多い。これは、鍵が解析されれば以後のデータは全て解読されてしまうために、鍵をさらに上位階層の鍵で暗号化することによって安全性を高めたり、用途の異なる鍵（署名用の鍵と暗号用の鍵等）を複数用いることによって、暗号と認証の機能を同時に実現する等のために行われるものである。この場合、暗号化を復号、署名、検証と用途に応じて置き換えれば種々の機能に対応する。
【０００５】図において鍵暗号化の最初となる鍵をマスタ鍵、直接データを暗号化する鍵をワーク鍵と呼び、それ以外の鍵は鍵暗号化鍵と呼ぶ。マスタ鍵を初めとする幾つかの鍵暗号化鍵は予めユーザに配送されている鍵であったり、誰でもがアクセスできる公開の鍵であったりする。また、ワーク鍵を初めとする幾つかの鍵暗号化鍵は送信者、受信者または鍵を管理するセンタ等がその場限りに設定した鍵であったり、鍵検索の手間を省いたり、送信者を特定するためにデータと共に送られる鍵であったりする。
【０００６】このような鍵は暗号化または署名したデータと共にかつ／または別に受信者に送られることが多い。よって、暗号・認証通信にはデータに関する通信の他に鍵に関する通信が存在する。そして、その通信に関する安全性は図６の上位の階層に関する通信の方がより重要であることは明らかである。なぜならば、上位の階層に関する通信が信頼できなければそれ以下の階層に関する通信は全て信頼できないためである。しかしながら、従来の通信において上位階層や下位階層に関する鍵情報とデータ情報を区別していなかったり、情報の位置等によって区別していても、情報の重要度という意味で区別して通信する方式は提案されていなかった。
【０００７】
【課題を解決するための手段】本発明は上述のような実情に鑑みてなされたものであり、情報やサービスの重要度といった特徴を生かすことのできる通信装置およびシ

ステムおよび方法を提供しようとするものである。
【０００８】この課題を解決するため、たとえば本発明の通信装置は以下に示す構成を備える。
【０００９】階層的に構成され、上位階層に属する鍵が下位階層に属する鍵またはデータを変換して通信を行う暗号・認証による通信通信であって、上位階層に関する該暗号・認証通信の品質がそれより下位の階層に関する該暗号・認証通信の品質より高くなるように、通信の品質を定める手段を有することを特徴とする。
【００１０】
【発明の実施の形態】以下、添付図面に従って本発明に係る実施形態の一例を詳細に説明する。
【００１１】先ず、本実施形態では、Ｂ－ＩＳＤＮにおいてはマルチメディアを扱うために各メディアで異なるトラフィック特性を許容する。そのために、メディア毎に異なるＱＯＳ（Quality Of Service：サービス品質）が要求される。ＡＴＭにおけるＱＯＳとしては遅延と遅延変動の感度、セルの損失率等が一式のパラメータとして定義されている（他のＱＯＳパラメータについては今後の検討課題）。
【００１２】ここで、遅延とはデータが発信されてから受信されるまでの時間であり、遅延変動は輻輳などによるセルの転送時間のバラツキである。映像伝送の場合、遅延変動はビットのゆらぎを引き起こすための受信側で十分なバッファメモリを持ってなければ画面がちらつくことになる。また、遅延が大きくなると会話用音声データのようにリアルタイム性が必要なものについては、エコーキャンセルなどの工夫が必要となる。逆にリアルタイム性の少ないテキストデータであれば、遅延は遅延変動と共に全く問題はない。セル損失率は、発信者により送出されるセルの総数と着信者に届かないセルの総数の比率を定義するものであり、データを垂れ流すタイプの映像伝送においては、フレーム落ちが起こったり、ノイズが出たりするので通信品質への影響は大きい。また、最近研究の進んでいるＭＰＥＧ等の予測符号化を基本とする圧縮方式では、さらに大きな画質劣化を引き起こし得るのは理解できよう。このように、ＱＯＳの各パラメータは用途によってその要求が異なる。
【００１３】ユーザとネットワーク間でのＱＯＳの要求・設定は次のように行われる。ユーザはネットワークが提供するＱＯＳクラス（幾つかのＱＯＳパラメータを組み合わせたもの）の中から、あるクラスのＱＯＳを要求する。これはトラフィック契約等とともに通常は通信の設定段階（可能な場合は通信途中でも再設定）で行われる。この時、ネットワークは要求されたトラフィックが実際の伝送容量を超えないかの判断をすると同時に要求されたＱＯＳクラスが確保できるか等を判断して、通信可能ならば端末に通知し通信モードに入る。通信モードにおいて、ユーザがトラフィック契約を遵守している限り、ネットワークは要求されたＱＯＳを維持し、要求された品質を保証する。
【００１４】また、通信においては種々のプロトコル（通信規約）が定められ、Ｂ－ＩＳＤＮのプロトコルでは、いろいろの機能の追加や変更が全体に影響を及ぼさないように、図７に示すようなプロトコルの階層化が行われている。各階層間では受け渡しの約束が決められており、個々の階層をレイヤと呼ぶ。図７において、物理レイヤは文字通り物理媒体に関する規定（ケーブル、コネクタの仕様の他に伝送フレームの構成、セル挿入、抽出機能を含む）であり、ＡＴＭレイヤは全てのサービスに共通なセルの多重化及び交換を行う。ＡＡＬ（ＡＬＴアダプション・レイヤ）は各サービスに依存する機能を扱い、各サービスに対応して複数のプロトコルが規定されている。このＡＡＬによって、各サービスに依存する上位レイヤの機能の追加、変更を吸収し、Ｂ－ＩＳＤＮの基本機能に影響を与えないようにしている。よって、各サービスが要求するＱＯＳの上述のＡＴＭのＱＯＳへの変換、及び逆変換は、ＡＡＬを含む上位レイヤで行われる。
【００１５】このように、Ｂ－ＩＳＤＮにおいてはＱＯＳを用いて通信の品質を指定することができる。
【００１６】よって、本実施形態では、このＱＯＳに図６の階層に応じた重要度（品質）を設定する、即ち、セル損失率等において上位階層に関する通信はそれ以下の階層に関する通信以上のＱＯＳの品質を設定する手段を有することによって暗号・認証通信の情報の重要度に応じた通信を実現するものである。
【００１７】図１に本発明の実施形態に対するフローチャートを示す。図において、階層に応じたＱＯＳをもつコネクションの開設を実現する手段として一例として図２に示すような前記のＱＯＳ要求・設定手順を行うＱＯＳ設定手段と、階層情報を受けそれに対応するＱＯＳをテーブルとして格納したＱＯＳ記憶手段によって構成できる。また、図１のフローチャートの全体の制御、及びその一部としての階層情報の出力はＣＰＵ等の制御手段によって行われる。ただし、図中の階層情報Ｋは図６の階層の総数に当り、最上位層をＫとし下位階層になるにつれて小さくなるとする。よって、通信要求が生じた時、図１の手段はまず階層情報をＫとして最も高品位のＱＯＳを要求・設定する。そのコネクションを用いて最上位のマスタ鍵による鍵暗号化鍵の暗号・認証通信を行う。図１の手段は該暗号・認証通信終了後コネクションを閉じる。その後、階層情報Ｋを１ずつ小さくして、その階層に応じたコネクションを再び要求・設定して前記の動作を繰り返し、Ｋ＝０となれば終了する。ただし、鍵の中にマスタ鍵と同様の通信を必要としない鍵がある場合は、コネクション開閉処理と暗号・認証通信は省略される。
【００１８】また、マスタ鍵以外に通信を必要としない鍵がない場合は鍵通信の必要性を判定する処理は省略さ

れる。また、幾つかの階層に亙ってＱＯＳが同じである場合は、コネクションの開閉に関する処理を階層毎に行う必要はない。これらの制御の変更は制御手段へのプログラミングの変更等によって容易に可能である。さらに、ＱＯＳ記憶手段がなくても階層に応じたＱＯＳを予めプログラミングしておく等によっても本発明は実現できる。また、階層に対して固定のＱＯＳでなくても、上位階層の場合にはその時点で要求できる最高のＱＯＳを要求する等の処理をしても良い。また、ＱＯＳは上位階層が下位階層に対して必ず高品位でなくても、ＱＯＳ記憶手段の設定やＱＯＳ設定手段のプログラミング等によって任意に設定することができる。ただし、図１の一連の通信（複数のコネクションにまたがる）は関連しているので、通信には他の通信を区別するために識別子のようなものを用いることができる。

【００１９】以上は、通信の設定段階でＱＯＳを定めるコネクション型の通信に対して有効である。

【００２０】＜第２の実施形態＞Ｂ－ＩＳＤＮでは種々のＱＯＳの他に、情報の転送に先立って通信を設定するコネクション型と、送信情報が発生した時点で相手に情報を通信するコネクションレス型などの様々なコネクション設定形態も提供している。前述の実施形態（第１の実施形態）はコネクション型の通信に対するものであった。本第２の実施形態では、通信途中でＱＯＳを変更できるコネクションレス型に対する場合を示す。

【００２１】図８にコネクションレス型のプロトコルの構成の一例を示す。図において、ＣＬＮＡＰ(Connectionless Network Access Protocol)は図７に示される上位レイヤの一部であり、コネクションレス型のプロトコルを実現するレイヤである。そのレイヤにおけるＰＤＵ(Protocol Data Unit)フォーマットは図９のように示される。ＰＤＵとはプロトコルを規定するデータ単位を示すものであり、ＳＵＤ(Service Data Unit)は、プロトコルを使用するユーザからのデータ単位である。この場合、ＱＯＳはＰＤＵのヘッダ中の４ビットのデータとして指定され、このＰＤＵはＣＬＮＡＰレイヤにおいて生成される。このＰＤＵをＡＡＬ、及びＡＴＭレイヤにおいてセル化または合成され、物理レイヤを介して送信される。よって、コネクションレス型ではＰＤＵ毎にＱＯＳを設定することができる。

【００２２】よって、コネクションレス型の通信プロトコルでは、階層毎（異なるＱＯＳ毎）に異なるＰＤＵを発生させ、そのＰＤＵに含まれる暗号情報の階層に応じてＱＯＳを設定することによって、情報の重要度（階層）に応じた通信を実現する。これは図１のコネクションをＰＤＵに置き換えた制御によって実現できる。

【００２３】図３に本第２の実施形態における構成概念図を示す。図示に示す暗号化手段は入力データを受けてそれを暗号化した情報をＱＯＳ設定手段に、階層情報をＱＯＳ記憶手段に送る。ただし、マスタ鍵等のユーザ毎の鍵は公知の鍵管理手段によって管理されているとするが、そうでない場合（外部のカード等から鍵を入力する場合など）、鍵は通信等を介して暗号化手段に入力される。また、ワーク鍵等のその場限りの鍵は公知の乱数生成手段や演算手段等を用いて生成される。また、それらの鍵による暗号化は公知の暗号処置手段によって実現され、出力される暗号情報はＱＯＳ設定手段に送られる。さらに、それらの鍵の使用順序は予め定められており、その使用順序が鍵の階層に相当するので、制御手段は予め定められた鍵の使用順序（階層）に基づき、前記鍵管理手段（または外部）からマスタ鍵等や前記乱数生成手段及び演算手段からワーク鍵等を前記暗号処理手段に与え、それに対応したデータの入力（ワーク鍵等がデータとなる場合もある）に応じて暗号化を行わせ、その処理順序を階層情報としてＱＯＳ記憶手段に送る。

【００２４】次に、ＱＯＳ記憶手段は階層情報に対応するＱＯＳをテーブルとして記憶する記憶手段によって構成され、入力された階層情報に応じたＱＯＳをＱＯＳ設定手段に与える。ＱＯＳ設定手段は出力データ（該暗号情報を含む所定の情報）に所定の位置かつ／または形式で該ＱＯＳを設定・出力する。

【００２５】次に、受信側に対する本実施形態を図４を参照にして説明する。

【００２６】受信側では、第１の実施形態に示した手段による通信を受けた場合を考える。図４において、ＱＯＳ分析手段は入力データを分解して、予め定められた情報の位置や識別信号等の形式から暗号情報と階層情報を分解して復号手段に送る。復号手段において制御手段はその階層情報が鍵管理手段に管理されている階層の情報であれば鍵管理手段からその鍵を検索して復号処理手段に入力し、その暗号情報を復号する。さらに、その復号結果が鍵として用いられる階層の情報であれば、その復号結果を鍵記憶手段に一時的に保持させる。また、制御手段はその階層情報が鍵管理手段で管理されていない階層の情報の場合は、保持された復号結果の中からその階層の鍵となる情報を検索してそれを鍵として復号処理手段に入力し、暗号情報を復号し出力させる。ただし、前記の復号結果をもとに演算手段によって鍵を生成する場合もある。よって、ＱＯＳ分析手段はＣＰＵ、ＤＳＰ等の処理手段やＲＡＭ等の記憶手段の組合せで実現でき、復号処理手段は第１の実施形態の暗号処理手段に対応する公知の復号処理手段、鍵管理手段は第１の実施形態と同様の手段、制御手段もＣＰＵ、ＤＳＰ等の処理手段によって実現でき、演算手段もまたＣＰＵ、ＤＳＰ等によって容易に実現できることは明らかである。

【００２７】以上は、暗号化及び復号について説明したが、認証が含まれている場合は暗号を署名、復号を検証と置き換えて処理すれば、認証通信に対しても同様の手段によって鍵の重要度に応じた通信が可能であることは明らかである。また、送信と受信を兼ねる装置の場合、

図３、４の構成要素は同様であるので図３，４の手段を合成させた手段（プログラム）を用いることも容易である。

【００２８】＜第３の実施形態＞第１、第２の実施形態においてはコネクション型、コネクションレス型の通信において情報の重要度に応じた通信を実現する手段を各々示した。本実施形態においては第１、第２の実施形態を含む情報の重要度に応じた通信を実現する通信システムについて図５を参照に説明する。

【００２９】ここでは一例として第１の実施形態における手段は図５の送信者端末、かつ／または受信者端末に各々内蔵されているとし、図６の階層において階層数Ｋ＝２、即ちマスタ鍵とワーク鍵の場合のみを考える。また、コネクション型の通信で、鍵とデータに関する暗号・認証処理は以下に示すＩＤ－ｂａｓｅｄ鍵共有方式によって行われる場合を考える。

【００３０】［ＩＤ－ｂａｓｅｄ鍵共有方式］鍵配送手段の管理を行うセンタが存在しており、各エンティティの名前や電話番号などの識別し（ＩＤ）をセンタが受け取り、センタ固有の秘密アルゴリズムを用いて、そのＩＤに対応する秘密鍵を生成して各エンティティに送り、各エンティティはその秘密鍵と通信相手の公開されているＩＤから共有すべき暗号鍵を計算して求める方式である。この方式は、ＩＤ－ｂａｓｅｄ鍵共有方式と呼ばれ、通信相手の確認と鍵の共有が同時に行える。

【００３１】この方式は大きく分けて暗号通信に先立つ呼び通信を必要とする方式としない方式に分類される。予備通信を必要とする方式は通信文のみを暗号化して送る電子メールのような使用ができないが、予備通信を必要としない方式は電子メール的な使用ができ、利用範囲が広い。しかし、予備通信を必要としない方式は多くのエンティティが結託した場合、センタの秘密が露呈するという問題がある。予備通信を必要とする方式としては岡本（栄）の鍵配送方式が良く知られており、予備通信を必要としない方式としては松本・今井の鍵配送方式がよく知られている（詳細は辻井，笠原著「暗号と情報セキュリティ」昭晃堂，１９９０．の第４章参照）。以下に、予備通信を必要とする方式の代表的として岡本（栄）の鍵配送方式を示す。

【００３２】岡本（栄）の鍵配送方式：

１）センタは一方向性関数として公開鍵暗号方式の１つであるＲＳＡ暗号を公開する。即ち、２つの素数ｐ，ｑ、及び復号鍵ｄを秘密に持ち、ｎ＝（ｐ・ｑ）、及び暗号鍵ｅを公開する（暗号鍵ｅと復号鍵ｄはｅ・ｄ＝１　ｍｏｄ（ｐ－１）・（ｑ－１）の関係をもつ）。さらに、同時に有限体ＧＦ（ｐ）とＧＦ（ｑ）の原始元ｇも公開する。

【００３３】２）各ユーザｊはネットワーク加入時に、センタに自分の識別子ＩＤｊを登録し、センタからＳｊ＝ＩＤｊｄ　ｍｏｄ　ｎを計算・送信してもらい、それを秘密に管理する。

【００３４】３）ユーザＡとユーザＢは鍵共有を行うとき以下のｉ～ｉｖような通信・計算を行う。

ｉ．ユーザＡは乱数ｋＡを任意に選び、ＣＡ＝ＳＡ・ｇｋＡ　ｍｏｄ　ｎをユーザＢに送る。

ii．ユーザＢは乱数ｋＢを任意に選び、ＣＢ＝ＳＢ・ｇｋＢ　ｍｏｄ　ｎをユーザＡに送る。

iii．ユーザＢはｙ＝（ＣＡｅ／ＩＤＡ）ｋＢ　ｍｏｄ　ｎ（＝ｇｅｋＡｋＢ　ｍｏｄｎ）を計算とする。

iv．ユーザＡはｙ＝（ＣＢｅ／ＩＤＢ）ｋＡ　ｍｏｄ　ｎ（＝ｇｅｋＡｋＢ　ｍｏｄ　ｎ）を計算とする。

【００３５】４）ユーザＡ，Ｂともにｙを共有鍵として暗号通信を行う。

【００３６】ここで、マスタ鍵は２）におけるＳｊに相当し、ワーク鍵は３）におけるｙに相当する。よって、２）のＳｊは予め各ユーザが有しており、３）の処理・通信が鍵に関する暗号・認証通信であり、４）がデータに関する暗号通信に相当する。また、ユーザＡは図５の送信者、ユーザＢは受信者に相当する。以下、図５の各端末は第１の実施形態に示す手段の他に、公知のＩＤ－ｂａｓｅｄ鍵共有手段を有しているとする（通常、前述のＳｊは該ＩＤ－ｂａｓｅｄ鍵共有手段によって管理されている）。

【００３７】先ず、ユーザＡはユーザＢと暗号・認証通信を行う時、先ずＫ＝２として第１の実施形態を用いてネットワークとＱＯＳの交渉を行い、ユーザＢとの間に高品位のＱＯＳをもつコネクションを開設する。コネクション開設後、ユーザＡはユーザＢとの間で公知のＩＤ－ｂａｓｅｄ鍵共有手段を用いて、３）の処理・通信を行い、互いにワーク鍵ｙを共有し、コネクションを一旦終了する。その後、Ｋ＝１として再びネットワークとＱＯＳの交渉を行い、ユーザＢとの間にＫ＝２の場合以下の品位のＱＯＳをもつコネクションを開設する。このコネクションを用いて、ユーザＢとの間でワーク鍵ｙによる暗号通信を実現する。

【００３８】次に、コネクションレス型の通信で、マスタ鍵は送信者と受信者で予め共有され、各々の鍵管理手段に格納されており、ワーク鍵は送信者の乱数生成手段で生成される乱数をそのまま用いる場合を考える。この場合、図５の端末は第２の実施形態を含む。

【００３９】送信者がデータをワーク鍵で暗号化して受信者に送るとき、先ず送信者は受信者と共有しているマスタ鍵を鍵管理手段から検索し、それによって乱数生成手段の出力であるワーク鍵を暗号化してその階層情報と共にＰＤＵを構成し、ＱＯＳ記憶手段からその階層に対応する高品位のＱＯＳを付けてＡＴＭセル化して受信者に送る。さらに、送信者はその乱数をワーク鍵としてデータを暗号化してその階層情報とともにＰＤＵを構成し、ＱＯＳ記憶手段からその階層に対応する前記のＱＯＳ以下の品位のＱＯＳを付けて同様にＡＴＭセル化して

受信者に送る。

【００４０】受信者はセルを合成したＰＤＵから暗号情報、階層情報、送信者、暗号化番号、暗号化の有無等を特定する。ただし、暗号化番号とはワーク鍵とその鍵で暗号化したデータを結び付けるために用いる情報である。よって、受信者は暗号化の有無、及び階層情報等から情報がマスタ鍵によって暗号化されている等を判断し、その場合送信者情報から共有しているマスタ鍵を検索する。さらに、それを鍵として暗号情報を復号し、それをワーク鍵をして暗号化番号と共に鍵記憶手段に保持する。そのＰＤＵが下位の階層に属する場合、暗号化番号が一致するワーク鍵を鍵記憶手段から検索しそれを鍵として暗号情報を復号し、送信者から送られたデータを入手する。

【００４１】以上のように、図５の通信システムは種々の鍵とデータに関する通信に適用できることがわかる。

【００４２】以上は、簡単のための例であるが、第１、第２の実施形態が外付けである場合、図６が多階層である場合、岡本（栄）のＩＤ－ｂａｓｅｄ鍵共有法以外の鍵共有法の場合、コネクション型の通信とコネクション型の通信が混在する場合等の各々に対しても同様の通信システムが実現できることは明らかである。また、図５の１つの端末を鍵に関するセンタ局として、送信者と受信者、及びセンタで図４のような階層構造をもつ暗号・認証通信を実現する場合にも、本実施形態が有効であることは明らかである。

【００４３】＜その他の実施形態＞前記の実施形態では情報の重要度に応じた通信を実現するためにＱＯＳを用いたが、通信の品位を実現する手段としてはＱＯＳに限定されず他の実現手段も本発明は含む。その実施形態においては図１～図４のＱＯＳに関する部分をその実現手段に置き換えることによって容易に実現できることは明らかである。

【００４４】なお、本発明は、上記処理を実現するための装置と通信端末が分離されていても、１つの機器からなる装置に適用してもよい。

【００４５】また、本発明の目的は、前述した各実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読出し実行することによっても、達成されることは言うまでもない。

【００４６】この場合、記憶媒体から読出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【００４７】プログラムコードを供給するための記憶媒体としては、例えば、フロッピディスク，ハードディスク，光ディスク，光磁気ディスク，ＣＤ－ＲＯＭ，ＣＤ－Ｒ，磁気テープ，不揮発性のメモリカード，ＲＯＭなどを用いることができる。

【００４８】また、コンピュータが読出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているＯＳ（オペレーティングシステム）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００４９】さらに、記憶媒体から読出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００５０】

【発明の効果】以上説明したように本発明によれば、情報の重要度に応じた通信を実現できる。特に、暗号化における鍵の階層に対応した通信品位を有する通信が実現できるようになる。

【００５１】

【図面の簡単な説明】

【図１】実施形態に対する処理手順を示すフローチャートである。

【図２】実施形態における処理構成の概念図である。

【図３】第２の実施形態における送信側の構成概念図を示す図である。

【図４】第２の実施形態における受信側の構成概念図を示す図である。

【図５】第３の実施形態における通信システムの構成を示す図である。

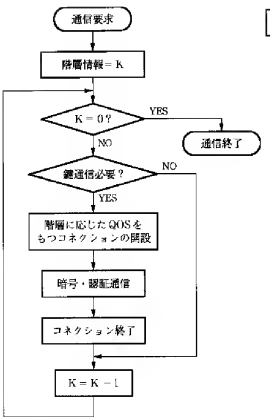
【図６】階層暗号化の概念図である。

【図７】実施形態におけるプロトコルの階層を示す図である。

【図８】第２の実施形態におけるコネクションレス型のプロトコルの構成の一例を示す図である。

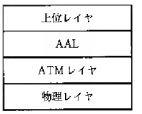
【図９】第２の実施形態におけるＰＤＵフォーマットを示す図である。

【図１】

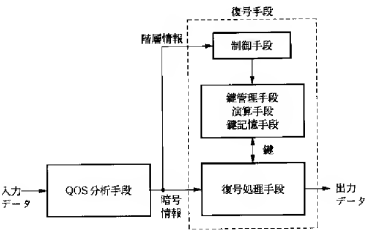


【図２】

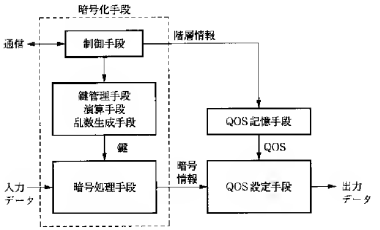
【図７】



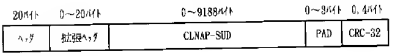
【図４】



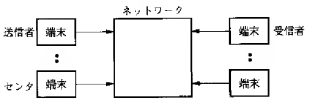
【図３】



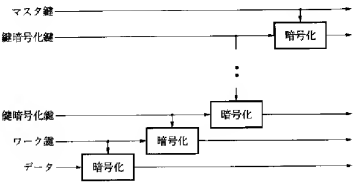
【図９】



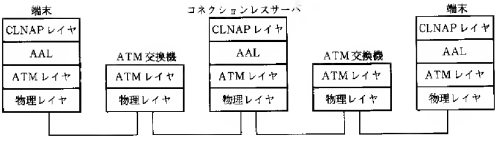
【図５】



【図６】



【図８】


端末
CLNAP レイヤ
AAL
ATM レイヤ
物理レイヤ
ATM 交換機
ATM レイヤ
物理レイヤ
コネクションレスサーバ
CLNAP レイヤ
AAL
ATM レイヤ
物理レイヤ
ATM 交換機
ATM レイヤ
物理レイヤ
端末
CLNAP レイヤ
AAL
ATM レイヤ
物理レイヤ